

UNITED STATES DISTRICT COURT
for the
District of Minnesota

In the Matter of the Search of
8840 Xerxes Circle South, Bloomington, Minnesota 55431, a
residential structure light brown/tan in color with dark trim

) CASE NO.

MJ 10-241 SRN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property

8840 Xerxes Circle South, Bloomington, Minnesota 55431, a residential structure light brown/tan in color with dark trim, described in more detail in Attachment A.

located in the State and District of Minnesota, there is now concealed

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is:

evidence of a crime;
contraband, fruits of crime, or other items illegally possessed;

The search is related to a violation of: Title 18, United States Code, Sections 2252(a)(1) and 2252(a)(4)(B), transportation and possession of child pornography

The application is based on these facts:

See Affidavit attached hereto and incorporated herein by reference.

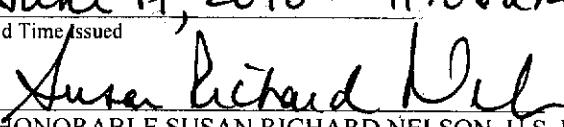
Continued on attached sheet.

Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


06/14/2010
Signature of Applicant
PAUL M. COUTURIER, Special Agent,
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence

June 14, 2010 11:06 am at
Date and Time Issued



THE HONORABLE SUSAN RICHARD NELSON, U.S. Magistrate Judge

Minneapolis, MN
City and State

SCANNED

JUN 29 2010

U.S. DISTRICT COURT ST. PAUL

STATE OF MINNESOTA)
) ss. AFFIDAVIT OF PAUL M. COUTURIER
COUNTY OF HENNEPIN)

I, Paul M. Couturier, being first duly sworn under oath,
depose and state as follows:

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI") and have been so employed for approximately two years. I am currently assigned to the Minneapolis, Minnesota, Division of the FBI and work on the Minnesota Cyber Crimes Task Force. As a member of the Cyber Crimes Task Force, my responsibilities include the investigation of various criminal offenses involving computers, computer networks, and the Internet, including the investigation of crimes involving the sexual exploitation of children. While employed by the FBI, I have participated in investigations in which evidence, in an electronic format, was seized.

BACKGROUND

2. The statements in this affidavit are based in part on information provided by Special Agents of the FBI, other law enforcement officers, and my experience and background as a Special Agent of the FBI.

3. Since this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, § 2252(a)(1) (transportation of a visual depiction involving the

use of a minor engaging in sexually explicit conduct) and Title 18, United States Code, § 2252(a)(4)(B) (possession of a visual depiction involving the use of a minor engaging in sexually explicit conduct) will be found at 8840 Xerxes Circle South, Bloomington, Minnesota 55431. This premises is more particularly described in Attachment A.

RELEVANT STATUTES

4. This investigation concerns alleged violations of Title 18, United States Code, Section 2252(a)(1) (transportation of a visual depiction involving the use of a minor engaging in sexually explicit conduct) and Title 18, United States Code, Section 2252(a)(4)(B) (possession of a visual depiction involving the use of a minor engaging in sexually explicit conduct):

Title 18, United States Code, Section 2252(a)(1) provides in pertinent part that:

Any person who knowingly transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction, if (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct . . . shall be [guilty of an offense against the United States].

Title 18, United States Code, Section 2252(a)(4)(B) provides in pertinent part that:

Any person who knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or

transported, by any means including by computer, if (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct . . . shall be [guilty of an offense against the United States].

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

5. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of child pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

6. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

7. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be downloaded directly into a computer.

8. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly

referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

9. Child pornographers can also reproduce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred, or printed out directly from the computer.

10. The captured images are similar to photographs. The images can be printed, edited, lightened, darkened, cropped, and manipulated in a wide variety of ways. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. There is added benefit to the child pornographer that this method of production does not leave as large a trail for law enforcement to follow as other methods.

11. Another method of which child pornographers are known to store and preserve their collection of images is on an external hard drive, commonly known as a pen drive, thumb drive, cruiser disk or USB drive. Such drives can be physically small in nature but have the capacity to store hundreds of images, movies or other digital media. The small size of the drives makes them compact and mobile in addition to making them easy to conceal.

12. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. Child pornography can be electronically mailed to anyone with access to a computer and modem. With the proliferation of commercial services and chat services, the computer has become one, if not the preferred, method of distribution of pornographic materials.

13. A computerized depiction of child pornography is often stored and referred to as a GIF, short for Graphic Interchange Format, or a JPEG, short for Joint Photographic Experts Group. These image files often contain images or photographs that have been converted into a computer format by the use of a scanner. A single image may be recorded as a single computer file. However, a file may contain two or more images (sometimes more than 100), and these files are often referred to as ZIP or SIT files referring to their compressed archive format. Another type of file is called an MPEG, short for Moving Picture Experts Group. An MPEG is a file containing a movie or video clip.

14. Previously, as a general matter, child pornographers had to rely on personal contact, U.S. Mail, and telephonic communications in order to sell, trade or market child pornography. The development of the computer has also changed that. A device known as a modem allows any computer to connect to another computer through the use of telecommunications lines. By connection to a

host computer, electronic contact can be made to literally millions of computers around the world.

15. A host computer is one that is attached to a network and serves many users. These host computers are sometimes commercial online services which allow subscribers access to a network which is in turn connected to their host systems. These service providers allow electronic mail service between subscribers and sometimes between their own subscribers and those of other networks or on the Internet. Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms."

16. Contact with others in this online format is very open and anonymous. The communication can also be quite private in the form of person-to-person instant messages. This communication structure is ideal for the child pornographer.

17. The open and anonymous communication allows the user to locate others of similar inclination and still maintain their anonymity. Once contact is established, it is possible to send messages and graphic images to a trusted person with similar interests. In addition to the use of large service providers, child pornographers can use standard Internet connections, such as those provided by businesses, universities, and government agencies to communicate with each other and distribute child pornography. These communication links allow contacts around the world in a relatively secure and anonymous format. These advantages are well

known, serving as a foundation of commerce between child pornographers.

18. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

19. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

20. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer

user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer contains peer to peer software, when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

21. Most individuals who collect child pornography are sexually attracted to children, their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences, including children. Child pornography collectors express their attraction to children through the collection of sexually explicit materials involving children as well as other seemingly innocuous material related to children.

22. These individuals may derive sexual gratification from actual physical contact with children as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collectors most cherished sexual fantasies involving children.

23. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially

nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica," which is defined as any material, relating to children, that serves a sexual purpose for a given individual. It is broader and more encompassing than child pornography, but at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his intent. It includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

24. Child pornography collectors reinforce their fantasies, often by taking progressive, overt steps aimed at turning the fantasy into reality in some or all of the following ways: collecting and organizing their child-related material; masturbating while viewing the child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity

to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self interest.

25. Child pornography collectors almost always maintain and possess their material in the privacy and security of their homes or some other secure location such as their vehicle(s) where it is readily available. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. The collector is aroused while viewing the collection and, acting on that arousal, he often masturbates thereby fueling and reinforcing his attraction to children. This is most easily accomplished in the privacy of his own home.

26. Because the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, the collector rarely, if ever, disposes of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase. Individuals who use a collection in the seduction of children or to document that seduction treat the materials as prized possessions and are especially unlikely to part with them. Even if a child pornography collector does delete files from his hard drive or

other electronic media, a computer expert can still retrieve those files using forensic tools.

PEER TO PEER FILE SHARING

27. A growing phenomenon on the Internet is peer to peer file sharing ("P2P"). P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. While there are several P2P networks currently operating, the most predominant is the Gnutella 1 network. There are several different software applications that can be used to access these networks but these applications operate in essentially the same manner.

28. To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the world-wide network for download, however, a user is not required to share files to utilize the P2P network.

29. A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, a list of the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to

download files simply conducts a keyword search. The results of the keyword search are displayed and the user then selects file(s) which he/she wants to download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event. Often times a forensic examiner, using these logs, can determine the IP address from which a particular file was obtained.

30. A person interested in sharing child pornography with others in the P2P network, need only place those files in his/her "shared" folder(s). Those child pornography files are then available to all users of the P2P network for download regardless of their physical location.

31. A person interested in obtaining child pornography can open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The keyword search would return results of files being shared on the P2P network that match the term "preteen sex." The user can then select files from the search results and those files can be downloaded directly from the computer(s) sharing those files.

32. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person that includes child pornography files in his/her "shared" folder is

hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography.

33. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it reduces the time it takes to download the file. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular internet connection during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

34. Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation.

35. Internet Protocol (IP) addresses are used to definitively identify a particular computer on the internet. When a computer

user visits a website on the internet, their IP address is visible to that website. Law enforcement entities, in conjunction with Internet Service Providers, have the ability to identify a user's IP address to a specific household or residence.

SEARCHES AND SEIZURES OF COMPUTERS

36. Based on your Affiant's knowledge, training and experience, and the experience of other law enforcement personnel, your Affiant knows that the search and seizure of evidence from computers commonly requires agents to seize most or all computer items (hardware, software and instructions), to be processed later by a qualified computer expert in a laboratory or other controlled environment. The reasons why this is true are set forth in the paragraphs below.

37. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, etc.) can store the equivalent of thousands of pages of information. When the user wants to conceal evidence of a crime, he or she might store it in random order with deceptive file names. This requires the searching investigators to examine all the stored data to determine whether it contains items authorized to be searched and seized under the warrant. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site at the time the search warrant is executed.

38. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and

software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from a destructive code embedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

39. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit (CPU). In cases where the evidence consists partly of graphics files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create or display the data (whether stored on hard drives or on external media)

40. In addition, the computer and its storage devices, the monitor, keyboard and modem, are all instrumentalities of the crimes of transmitting and receiving child pornography within the meaning of Title 18, United States Code, Section 2252, and should be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

41. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or performing any other

data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

OVERVIEW OF INVESTIGATION

42. On July 27, 2009, Special Agent Stacie Lane (SA Lane), using a computer connected to the Internet, utilized a publicly available P2P file sharing program from the Innocent Images Operations Unit of the FBI, located in Calverton, Maryland. SA Lane logged on with a username that was obtained by an ID takeover, and she observed that an individual using the screen name "Anonymousmenu" was logged onto the P2P network.

43. SA Lane observed that Anonymousmenu was sharing over 21,000 files and that many of the image files depicted images of child pornography. The video files being shared by Anonymousmenu had titles that were indicative of child pornography. SA Lane selected 84 image files and 5 video files and downloaded them directly from Anonymousmenu's computer between 1:29 PM EDT and 2:07 PM EDT on July 27, 2009. During the download of these files, SA Lane used a software utility in order to identify the IP address of Anonymousmenu's computer, which was 75.72.10.104.

44. All of the image and video files downloaded by SA Lane depicted child pornography. In addition, several of the files depicted minors being subjected to bondage and bestiality. Among the files downloaded by SA Lane were the following eight files briefly described below:

- a) !!!!!babyfuck5.jpg - Image depicts a prepubescent boy naked from the waist down with an adult penis against his buttocks. There appears to be semen on the boy's buttocks.
- b) 028 (7).JPG - Image depicts a naked prepubescent boy being anally penetrated by an adult male.
- c) 7092935bls.jpg - Image depicts a prepubescent boy performing oral sex on an adult male.
- d) cum belly006.jpg - Image depicts a naked prepubescent boy lying down and exposing his genitalia. There appears to be semen on the boy's stomach and genitalia.
- e) MkBy0162.JPG - Image depicts a naked prepubescent boy. There is a dog licking the boy's penis.
- f) Babyj 5yo fucked 1-41.avi - This file is a video approximately 1 minute and 28 seconds long and depicts an adult male vaginally penetrating a prepubescent girl.
- g) ((Hussyfan)) (Pthc) -K- K !!!New - 5Yo Rca (Marissa) - Young Girl Lolita Pedo Fuck Brother.avi - This file is a video approximately 2 minutes and 30 seconds long and depicts a prepubescent girl performing oral sex on an adult male. The video further depicts the adult male rubbing his penis on the girl's buttocks and genitalia.
- h) Pedoland Babyj-Blue-Shot.avi - This file is a video approximately 38 seconds long and depicts an adult male anally penetrating a prepubescent girl.

45. Additionally, SA Lane also captured thumbnail images of over 4,900 image files. Most of the thumbnail images depict prepubescent children engaged in sexually explicit conduct.

46. SA Lane determined that IP address 75.72.10.104 was registered to the Internet Service Provider Comcast Communications (Comcast). Results from an administrative subpoena sent to Comcast on July 31, 2009, for the date and time the files were downloaded revealed that at that day and time the IP address was assigned to the account registered to Karen Sonday at 8840 Xerxes Circle South, Bloomington, Minnesota 55431, that the account/service began on July 29, 2005, and that the account status was currently active.

47. On January 22, 2010, SA George W. Howell from the FBI Richmond, Virginia office, using a computer connected to the Internet, utilized a publicly available P2P file sharing program. SA Howell observed that an individual using the screen name "Anonymousmenu" was logged onto the P2P network, and was sharing 144 files. SA Howell browsed Anonymousmenu's shared folders and observed files depicting images of child pornography and video titles indicative of the same. SA Howell subsequently downloaded ten videos from Anonymousmenu. The IP address used by Anonymousmenu was 75.72.10.104. SA Howell determined that the 75.72.10.104 IP address is assigned to Comcast Corporation. On January 27, 2010, the administrative subpoena to Comcast Corporation for IP address 75.72.10.104 showed subscriber information as Karen Sonday at 8840 Xerxes Circle South, Bloomington, MN 55431.

48. All of the video files downloaded by SA Howell depicted child pornography. Among the files downloaded by SA Howell were the following ten files briefly described below:

- a) !!NEW!!Beauty-Slurping.mpg - Video depicts a nude prepubescent girl performing oral sex on an adult male.
- b) (New)4Yo Loves It Aug2006.mpg - Video depicts a nude prepubescent girl sitting on the lap of an adult male. Her legs are spread, and the male is spreading her vagina.
- c) (pthc) 2009 Boy_and_girl.avi - Video depicts a young girl and a prepubescent boy licking each other's genitals. The boy penetrates the girl's vagina.
- d) [MB] New 2009!Nice_Cut(new_vid_finally).avi - Video depicts a prepubescent boy being stripped and touched by an adult male.
- e) 8Yo Deep T Good K.avi - Video depicts a prepubescent girl performing oral sex on an adult male.
- f) BABYJ_GOD.MPG - Video depicts a nude prepubescent girl, with her legs spread and bound. An adult male is vaginally and anally penetrating the girl.
- g) BEAUTIFUL_Venezuela-girls(3-4yo)part-2) pthc hussyfan_Pedo FuX Makes A Childs Cute Peepee Orgasm'.mpg - Video depicts two nude prepubescent girls, in a bath tube. An adult male is having oral and anal sex with the girls.
- h) Cambodian Brothel Real Stuff.avi - Video depicts three nude prepubescent girls spreading their legs and exposing and

touching their genitals. One of the girls performs oral sex on an adult male.

i) Cums - Honey Bee.mpg - Video depicts an adult male performing oral sex on a boy until the boy ejaculates.

j) Kid's 10 y hole widened and beiing fucked violently by two adults (14,50).avi - Video depicts a nude prepubescent boy being held by one male as another male uses his fingers and penis to anally penetrate the boy.

49. On April 14, 2010, SA Howell, from the FBI Richmond, Virginia office, using a computer connected to the Internet, utilized a publicly available P2P file sharing program. SA Howell observed that an individual using the screen name "Anonymousmenu" was logged onto the P2P network, and was sharing 22,273 files. SA Howell browsed Anonymousmenu's shared folders and observed files depicting images of child pornography and video titles indicative of the same. SA Howell subsequently downloaded four images and one video from Anonymousmenu. The IP address used by Anonymousmenu was 75.72.10.104. SA Howell determined that the 75.72.10.104 IP address is assigned to Comcast Corporation. On April 23, 2010, the administrative subpoena to Comcast Corporation for IP address 75.72.10.104 showed subscriber information as Karen Sonday at 8840 Xerxes Circle South, Bloomington, MN 55431.

50. Three images and one video clip downloaded by SA Howell depicted child pornography. Four of the files downloaded by SA Howell are briefly described below. In addition to the below four files, SA Howell previewed over 100 thumbnail images. The majority

of these previewed thumbnail images appeared to be child pornography.

a) a126491_138_psqco.jpg - Image depicts a standing nude adult male, with two nude prepubescent girls. One girl is performing oral sex on the man, while the other girl is holding the man's genitals.

b) good sound-Boy fucked hard (103).avi - The video clip depicts a nude prepubescent boy being anally penetrated by a nude adult male.

c) TB_Misha-006.jpg - Image depicts a nude prepubescent boy performing oral sex on a nude adult male.

d) TB_Misha-008.jpg - Image depicts a nude prepubescent boy with his legs spread and his genitals exposed. A nude adult male has his penis by the boy's anus.

51. In October 2009, various records indices were searched for information regarding Sonday and the user name Anonymousmenu.

a. Public records report accessed through Lexis Nexis, a public records database that can be accessed and searched over the Internet, for Sonday , shows a full name of Karen L. Sonday, and a social security account number xxx-xx-0778, date of birth xx/xx/1962, and shows an active address of 8840 Xerxes Circle South, Bloomington, Minnesota 55431. Additionally, Lexis Nexis showed Sean M. Kratz (Kratz), social security account number xxx-xx-6903, date of birth xx/xx/1990, to also have an active address of 8840 Xerxes Circle South, Bloomington, Minnesota 55431. The first five digits of the social security account numbers, and the month

and day of the dates of birth has been redacted for the purposes of this affidavit.

b. Department of Motor Vehicle records indicate that Sonday currently has two vehicles registered at 8840 Xerxes Circle South, Bloomington, Minnesota 55431, with the registrations expiring in July and September of 2010.

c. A Google search for Sonday showed her to be affiliated with the Sonday Reading Center in Edina, Minnesota. A review of the website <http://sondayreadingcenter.org> listed Karen Sonday as having a masters degree in special education.

52. A records check conducted with the Minnesota Department of Economic Security showed that both Karen Sonday and Sean Kratz were employed by the Sonday Reading Center as of the third quarter of 2009.

53. On October 27, 2009 and on April 30, 2010, the United States Postal Inspection Service confirmed that Karen Sonday and Sean Kratz receive mail at 8840 Xerxes Circle South, Bloomington, Minnesota 55431.

54. On October 23, 2009, a physical surveillance of 8840 Xerxes Circle South, Bloomington, Minnesota 55431, was conducted. This residence is described as a residential structure light brown/tan in color with dark trim. While facing the residence from the street the numerals "8840" are affixed vertically to the structure to the right of the front entrance and are plainly and clearly visible. To the right of the front entrance there is a driveway leading to a garage. To the left of the front entrance the residence appears to be of a split level style.

55. On May 10, 2010, a physical surveillance of 8840 Xerxes Circle South, Bloomington, Minnesota 55431, was conducted. At approximately 7:45 a.m., a female matching the description of Karen Sonday exited the home with a dog. She walked the dog down the street and returned home at approximately 7:50 a.m. At approximately 7:56 a.m., she was seen exiting Xerxes Circle South in a Honda CRV, license plate 408BAN. A DVS check indicated that the plates belong on a green Honda CRV registered to Karen Sonday at 8840 Xerxes Circle South, Bloomington, Minnesota 55431.

CONCLUSION

56. Based on the aforementioned factual information, your Affiant respectfully submits that there is probable cause to believe that contraband, evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(1) (transportation of a visual depiction involving the use of a minor engaging in sexually explicit conduct) and Title 18, United States Code, Section 2252(a)(4)(B) (possession of a visual depiction involving the use of a minor engaging in sexually explicit conduct) will be found at the premises located at 8840 Xerxes Circle South, Bloomington, Minnesota 55431.

57. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the premises described further in Attachment A and seizure of the items described further in Attachment B consistent with the procedure set forth herein and in the Search Warrant Addendum attached hereto.

Further your Affiant sayeth not.

PMC 06/14/2010
Paul M. Couturier
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me

this 14th day of June, 2010.

Susan Richard Nelson

HON. SUSAN RICHARD NELSON
United States Magistrate Judge

ATTACHMENT A

8840 Xerxes Circle South, Bloomington, Minnesota 55431 is described as a residential structure light brown/tan in color with dark trim. While facing the residence from the street the numerals "8840" are affixed vertically to the structure to the right of the front entrance and are plainly and clearly visible. To the right of the front entrance there is a driveway leading to a garage. To the left of the front entrance the residence appears to be of a split level style.

ATTACHMENT B

1. Internet billing and use records.
2. Records or other items that evidence ownership or use of computer equipment found in the premises to be searched, including, but not limited to, sales receipts, handwritten notes and handwritten notes in computer manuals.
3. Records evidencing occupancy or ownership of the premises to be searched, including, but not limited to, utility and telephone bills, mail envelopes, and/or addressed correspondence.
4. Any and all visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, in any format or media, including, but not limited to, undeveloped photographic film, photographs, magazines, videotapes, slides, and motion picture films.
5. Correspondence, books, ledgers, and/or records pertaining to the possession, receipt, distribution, transportation, or advertisement of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail.
6. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
7. Computer(s) and all related computer equipment, including scanners, peripherals, related instructions in the form of manuals, as well as the software used to operate the computer(s), and any CD-ROMS, zip disks, floppy disks, DVDs, memory cards, and other magnetic storage devices. The subsequent forensic analysis of these items is to be focused on searching for the items described in paragraphs 1-6 above.

SEARCH WARRANT ADDENDUM

1. In conducting the search authorized by this warrant, the government shall make reasonable efforts to utilize computer search methodology that avoids searching files, documents or other electronically stored information which is not identified in the warrant.

2. If electronically stored data or documents have been identified and seized by the government pursuant to this warrant, the government may retain the original hard drive or other data storage mechanism. The person from whom the data storage device has been seized may request that the government provide him or her with electronic copies of the electronically stored data or documents by making a written request to the United States Attorney's Office, identifying with specificity the files, data, or software sought to be copied. The government must respond to all such requests within a reasonable amount of time, and must provide a copy of the electronically stored data or documents requested unless the copies requested constitute contraband, instrumentalities, or property subject to forfeiture.

3. Nothing in this warrant shall limit or prevent the government from seizing the computer as contraband or an instrumentality of a crime or commencing forfeiture proceedings against the computer and/or the data contained therein. Nothing in this warrant shall limit or prevent the owner of the computer from (a) filing a motion with the Court pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure for the Return of Property or (b) making a request of the government to return certain specified files, data, software or hardware.

4. The government shall establish a search methodology governing the review of seized data to ensure that no attorney-client privileged communications will be inadvertently reviewed by the prosecution team. In the event that documents or other records seized pursuant to this warrant are identified by the government as possibly containing attorney-client privileged communications, an Assistant United States Attorney, who is not a member of the prosecution team and who is not participating in the search, shall act as a "taint team" to set up a "Chinese wall" between the evidence and the prosecution team that will prevent any privileged material from getting through.